Micro Focus
Fortify Software Security Content
2018 Update 3
2018年9月28日

Micro Focus Fortifyソフトウェアセキュリティリサーチについて

Fortifyソフトウェアセキュリティリサーチチームは、最先端の研究に基づいて、Fortify製品ポートフォリオ向けのセキュリティインテリジェンスを提供します。対象製品としては、Fortify Static Code Analyzer (SCA)、Fortify WebInspect、Fortify Application Defenderがあります。現在、Micro Focus Fortify Software Security Contentは、991の脆弱性カテゴリを25のプログラミング言語にわたってサポートし、1,007,000種類を超える個別のAPIに対応します。

詳細情報

https://software.microfocus.com/en-us/software/security-research

Fortifyソフトウェアセキュリティリサーチ (SSR) は、Fortify Secure Coding Rulepacks (英語版、バージョン2018.3.0)、Fortify WebInspect SecureBase (SmartUpdateを通じて入手可能)、Fortify Application Defender、Fortify Premium Content向けのアップデートが利用可能になったことをお知らせします。

Micro Focus Fortify Secure Coding Rulepacks [SCA]

Fortify Secure Coding Rulepacksのこのリリースでは、25種類のプログラミング言語にわたる788の固有の脆弱性カテゴリの検出が可能で、1,007,000種類以上の個別APIに対応します。リリース内容の概要を以下に示します。

YAML文書の安全でない逆シリアル化

複数の言語 (Java、Python、JavaScript、C#) のYAMLライブラリ向けに、新しいカテゴリである「動的コード評価: 安全でないYAML逆シリアル化」を検出するためのサポートが追加されました。この新しいカテゴリは、7つのライブラリにわたるAPIが対象で、信頼されないYAML文書を逆シリアル化する際に任意のコードが実行される可能性につながります。

パスの操作: Zipエントリの上書き

アーカイブおよび圧縮ライブラリの使用を通じて導入される脆弱性が最近注目されていることから、同様のリスクがどこに存在するかを理解するためにさらに詳しい研究が実施されました。新しいサポートでは、既存の「パスの操作: Zipエントリの上書き」カテゴリへの更新が行われ、対応する言語の数が増えるとともに、Javaに関する精度が向上しました。サポートは21種類のライブラリを対象とし、対応する言語はC#、Java、JavaScript、Objective-C、Python、Scala、Swiftです。

Python MongoDB

PyMongo Pythonライブラリのサポート。PyMongoは、MongoDBを操作するためのツール群であり、PythonからMongoDBを操作するための推奨される方法です。サポートされるカテゴリは以下のとおりです。

- DoS攻撃: 正規表現
- 動的コード評価: コードインジェクション
- NoSQLインジェクション: MongoDB
- パスワード管理: 空のパスワード
- パスワード管理: ハードコードされたパスワード
- 認証されていないサービス: MongoDB

OGNL式インジェクション: Struts 2

JavaでのApache Struts 2に関連したOGNLインジェクションのサポートが拡張されました。これは、リモートコード実行を可能にしたCVE-2018-11776のリリースを受けたものです。Apache Struts2バージョン2.3.x (2.3.34まで) またはバージョン2.5.x (2.5.16) を使用しているアプリケーションでは、名前空間なしまたはワイルドカード名前空間に設定されたアクション結果が含まれており、かつstruts構成でstruts.mapper.alwaysSelectFullNamespaceプロパティがtrueに設定されていると、攻撃者が任意のOGNL式を実行できます。

Java 9 API[1]

プロセスやスタックウォーキングなどの新しいJava 9 APIのサポートが導入されました。さらに、Stream、Optional、CompletableFutureクラスなどの改良されたAPIに対するカバレッジの拡張が導入されました。

[1] Java 9のサポートには、Fortify SCAバージョン18.20以降が必要です。

DISA STIG 4.7

コンプライアンスの分野で連邦政府のお客様をサポートするため、Micro Focus Fortifyの分類と、Defense Information Systems Agency (DISA) Application Security and Development STIG (バージョン4.7) の相関が追加されました。

Micro Focus Fortify SecureBase [Fortify WebInspect]

Fortify SecureBaseでは、何千もの脆弱性のチェックと、SmartUpdateを通じてただちに入手できる以下のアップデートに関してユーザーをガイドするポリシーが結び付けられています。

脆弱性のサポート

クロスサイトスクリプティングに関する機能拡張[2]

HTMLなしのXSSと呼ばれ、Angular JSテンプレートのインジェクションを通じてWebアプリケーションが危害を受ける可能性があります。Knockoutフレームワークのスクリプトガジェットによっても同様の脅威が発生します。このリリースでは、既存のパターンに対するサポートが拡張され、強化されたクロスサイトスクリプティング検出アルゴリズムが導入されました。これは、Angular JSおよびKnockout JSフレームワーク固有のクロスサイトスクリプティングおよびテンプレートインジェクションパターンに関してアプリケーションを評価します。

Webサーバーの構成の誤り: 安全でないマッピングディレクティブ

NGINXのロケーションエイリアスディレクティブは、指定したロケーションの置き換えを定義します。ただし、スラッシュで終わるロケーションマッピングを使用すると、攻撃者がアプリケーションサーバー上の秘密のリソース (制限されたフォルダー、構成ファイル、アプリケーションのソースコードなど) に不正にアクセスできる可能性があります。これには、Webルートの外に保存されているコンテンツが含まれます。新しいチェックでは、NGINX構成のこのような脆弱性を検出します。

安全でないデプロイメント: パス正規化の競合

1つのURLパスには、複数の代替URL表現が存在する場合があります。正規化プロセスの目的は、URLを特定の形式に変換することで、意味的に同一のURLのすべての構文バリアントが同じ方法で扱われるようにすることです。マルチレイヤー型のアーキテクチャーでは、クライアント要求がさまざまな中間コンポーネント (ロードバランサー、リバースプロキシ、Webアプリケーションファイアウォールなど) を通じてルーティングされるため、正規化が各レイヤーで異なる危険性があります。この場合、攻撃者は、ホワイトリストやブラックリストのACLルールを迂回したり、コンテキストマッピングを回避したりできる可能性があります。その結果、サーバー上の秘密のリソースが意図に反して公開されるおそれがあります。このリリースには、このような問題を特定するチェックが含まれています。

クロスサイトWebSocketハイジャック[3]

WebSocketの接続確立時に認証と接続要求の発信元チェックが不十分だと、WebアプリケーションがWebSocketハイジャックと呼ばれる重大な脆弱性の影響を受けます。攻撃者は、この脆弱性を利用することで、正当なユーザーになりすまし、認証されたユーザーとして秘密情報に対する要求を送信できます。このリリースには、WebSocketを利用してサイトの機能を実現しているアプリケーションのクロスサイトWebSocketハイジャックの問題を検出するチェックが含まれています。

---

[2] クロスサイトスクリプティング機能拡張のサポートには、Fortify WebInspect 18.20以降が必要です。

[3] クロスサイトWebSocketハイジャックのサポートには、Fortify WebInspect 18.20以降が必要です。

OGNL式インジェクション: Struts 2

今月初めに、WebInspect SecureBaseは、CVE-2018-11776で識別されるStrutsの重大な脆弱性を検出するチェックをリリースしました。リリース時にお客様にお伝えしたように、IBM WebSphere上にホストされたアプリケーションでは、IBM WebSphereでの特殊文字の処理方法が原因で、検出漏れが生じる可能性がありました。今回のリリースに含まれるチェックの機能強化により、この制限が解決されます。

安全でないトランスポート: Perfect Forward Secrecyの欠如

Perfect Forward Secrecy (PFS) とは、盗聴されたクライアントとサーバーの間の通信に対する将来の攻撃に対するセキュリティを、秘密キーが漏洩した場合でも確保する仕組みです。PFSを有効にするには、サーバー上でDiffie-Hellman Ephemeral (DHE) またはElliptical-Curve Diffie-Hellman Ephemeralベースの暗号化スイートを選択する必要があります。WebInspectでは、サーバーがSSLハンドシェークプロセス中にDHEまたはECDHEベースの暗号化スイートの選択肢を提供しなかった場合に、PFS脆弱性があると判定していました。ただし、新しい研究によれば、PFSを保証するためにはサーバーがDHEまたはECDHE以外の暗号化の選択肢を提供してはならないとされています。このリリースでの更新されたチェックでは、SSLハンドシェーク中にPFSのない暗号化スイートが選択肢として提示された場合に、脆弱性があると判定するようになっています。

コンプライアンスレポート

DISA STIG 4.7

コンプライアンスの分野で連邦政府のお客様をサポートするため、このリリースには、WebInspectのチェックと、Defense Information Systems Agency Application Security and Development STIGの最新バージョン (バージョン4.7) の相関が含まれています。

ポリシーの更新

WebInspect SecureBaseでサポートされるポリシーの既存のリストに、DISA STIG 4.7に関連するチェックを含むようにカスタマイズされたポリシーが追加されました。

Micro Focus Fortify Application Defender

Fortify Application Defenderは、ランタイムアプリケーションセルフプロテクション (RASP) ソリューションであり、自社製またはサードパーティ製のアプリケーションによるリスクの管理と軽減に役立ちます。アプリケーションの使用と悪用を集中的に可視化するとともに、ソフトウェアの脆弱性の利用やその他の違反からの保護をリアルタイムで実現します。このリリースで、Micro Focus Fortifyソフトウェアセキュリティリサーチチームは以下の機能改良を行っています。

パスの操作: Zipエントリの上書き

Zipファイルの処理に関連する既知の弱点をサポートする新しいルールが追加されました。一部のライブラリでは、ファイルを親ディレクトリに展開することが許可される場合があります。新しいルールで攻撃が検出されるJavaライブラリは、java.util.zip、Apache commons-compress、zip4j、codehaus/plexus-archiver、zeroturnaround/zt-zipです。

Micro Focus Fortify Premium Content

Fortifyソフトウェアセキュリティリサーチチームは、Micro Focusのコアセキュリティインテリジェンス製品以外にも、さまざまなリソースの作成、拡張、保守を行っています。

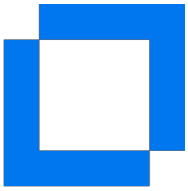
DISA STIG 4.7

新しい相関に関連して、このリリースには、DISA STIG 4.7をサポートする新しいレポートバンドルも含まれています。これは、FortifyカスタマーサポートポータルのPremium Contentの下からダウンロードできます。

Micro Focus Fortifyの分類: ソフトウェアセキュリティエラー

Fortify Taxonomyサイトには、新しく追加されたカテゴリサポートの説明が記載されています。このサイトには https://vulncat.fortify.com からアクセスできます。前回サポートされた更新が記載された旧サイトをお探しの場合は、Micro Focus Fortifyサポートポータルから入手できます。

Fortifyテクニカルサポート連絡先
Micro Focus Fortify
https://softwaresupport.softwaregrp.com/
+1 (844) 260-7219



SSR連絡先
Alexander M. Hoole
Micro Focus Fortify
ソフトウェアセキュリティリサーチ
担当マネージャー
hoole@microfocus.com
+1 (650) 258-5916

2018年9月28日